10/12/2010

www.enisa.europa.eu

La sécurité, existe-t-il une application pour cela ? L'agence européenne chargée de la cyber-sécurité met en évidence les risques et opportunités des Smartphones

Un nouveau rapport de l'ENISA identifie les principaux risques et opportunités de l'utilisation des Smartphones et donne des conseils de sécurité pratiques aux entreprises, aux particuliers et aux gouvernements. Les risques principaux incluent les logiciels espions, la mauvaise qualité du nettoyage de données lors du recyclage des téléphones, les fuites de données accidentelles et les appels téléphoniques et envois de SMS non autorisés à des tarifs majorés.

Les ventes mondiales de Smartphones ont doublé l'année dernière (d'après Gartner) et 80 millions d'appareils ont été vendus dans le monde entier, rien que pendant le troisième trimestre 2010 : le nouveau rapport de l'ENISA sur les risques et opportunités de sécurité des Smartphones arrive donc au moment opportun. Si vous figurez parmi les centaines de millions d'utilisateurs de Smartphone au monde, vous consacrez probablement plus de temps à votre téléphone qu'à votre conjoint : avec sa myriade d'applications et de capteurs, il en sait peut-être même encore plus sur vous. Ces nouveaux partenaires pour la vie constituent aujourd'hui un outil essentiel à travers toutes les sections de la société, des principaux dirigeants politiques aux chefs d'entreprise, en passant par les particuliers. Ils sont célèbres pour la diversité de leurs fonctions ; un Smartphone peut être un portefeuille sans contact, un appareil photo ou un visiophone, un lecteur de codes barres, une plateforme de courrier électronique, ou un moyen d'accéder aux réseaux sociaux.

«*Compte tenu de l'importance croissante des Smartphones pour les entreprises, les gouvernements et les citoyens de l'UE, nous considérons qu'il est essentiel d'évaluer leurs implications en termes de sécurité et de confidentialité*», explique le Prof. Dr. Udo Helmbrecht, Directeur Exécutif de l'ENISA.

Dans son nouveau rapport, l'ENISA analyse les risques et opportunités de sécurité clés. Certains de ces risques clés sont les suivants:

- Fuites accidentelles de données sensibles - ex.: via des données GPS attachées à des images.
- Vols de données par des applications malveillantes et depuis des téléphones volés, perdus ou mis hors service.
- «Diallerware» - un type de logiciel malveillant qui vole de l'argent en passant des appels téléphoniques non autorisés.
- Surcharge de l'infrastructure de réseau par les applications de Smartphones.

En termes d'opportunités, les fonctions de sauvegarde sont souvent très bien intégrées au sein des plateformes de Smartphones, ce qui facilite la récupération des données en cas de perte ou de vol de l'appareil. Une autre opportunité réside dans l'utilisation des boutiques d'applications en ligne (app-stores) : «*En règle générale, les utilisateurs de Smartphone n'installent de logiciels de tiers qu'au travers de circuits de distribution de logiciels contrôlés*», indique le Dr. Marnix Dekker, co-auteur du rapport.

Le résultat le plus important du rapport est une série complète de stratégies de sécurisation des Smartphones. «*Les Smartphones sont une mine d'or d'informations sensibles et personnelles et il est donc crucial de comprendre comment maintenir notre contrôle sur ces données. Nous avons élaboré nos recommandations pour qu'elles puissent être directement appliquées au sein d'une politique de sécurité typique*», ajoute en effet le Dr. Giles Hogben, co-auteur du rapport. Le rapport offre des recommandations s'adressant aux entreprises, aux hauts responsables et aux particuliers, tout en indiquant comment aborder les risques de sécurité impliqués dans le mélange de ces rôles.

Consultez **le rapport complet**.

Video

Document supplémentaire : **FAQ sur la sécurité des Smartphones**

Pour toute demande d'interview, veuillez contacter : Ulf Bergstrom, porte-parole de l'ENISA, press@enisa.europa.eu, portable : +30-6948-460143, ou pour tout complément d'information : le Dr Marnix Dekker, marnix.dekker@enisa.europa.eu.

Traduction. La version anglaise est la seule version officielle.